Microsoft® Windows 2000 FAQ Sheet For the State of Washington

Microsoft Corporation

INTRODUCTION

This document is a reply to the questions posed by the Windows 2000 steering committee for the State of Washington. This is the first round of responses in a living document that is open for distribution. The following is how the questions and answers will be formatted:

This is an example of the FAQ Answer formatting:

G This is an example of the general response

T This is an example of the technical response (if applicable)

B This is an example of the business response (if applicable)

:

Questions:

1. In a single forest environment, how will agencies be able to protect themselves against mistakes made by other agencies?

G - By having domain separations, there is almost no chance of an administrator from another domain causing any damage to a domain outside of their own. The largest chance for an error to occur is from the schema administrators group and the Enterprise Administrators. Both of these groups should be tightly controlled and limited to only trained personnel with a strong business reason to be in that group. There also is the Built-in Administrators (BA) group in the forest root domain, because the group can add themselves to the other two groups. Procedures are available to limit the three groups' access to other domains by revoking the appropriate ACLs.

2. How does Disaster/recovery work in the Active Directory environment?

B - The domain controller design will address the number and placement of DCs so that a machine can go down or be taken down when needed. With a correct design, there will be no service interruption while the recovery takes place.

G – There are three AD recovery scenarios: crashed DC (replaced or rebuilt—this scenario also includes an upgraded hardware platform), DC offline for a while then back on (power failure or memory upgrade), and an object deleted from the AD that must be restored.

In the first two cases, the recovery procedure is basically the same. The machine is built or rebuilt, and the latest tape image is applied to the DC. This will bring the AD database to the state it was in as of the latest backup. To get it current, simply turn it on and let it begin communicating with the other DCs on the net. The rebuilt DC will exchange USNs (update sequence numbers) with its counterparts and rebuild its AD database the rest of the way automatically.

In the case of a DC brought down for a while, then brought back up, the DC will communicate with its counterparts automatically and bring its copy of the directory up to date without any intervention required.

In the third case, someone deleted an AD object (OU, for example, yikes!) and we need to get it back. For this to work you need two things: a tape or other image of the database that has the deleted object on it, and the knowledge of how to do an authoritative restore.

Here's a little background: The Active Directory is a database that is replicated to every DC in the enterprise (not every component of the AD database is replicated to every DC but for our purposes here we can say this). Because there is a time lag in the replication, deleted objects have to be handled a little differently than created objects or objects whose properties have changed. When an AD object is created, the object is essentially copied to all the DCs. When an object's properties are changed, the changed properties are copied to all instances of that object on every DC. This takes some time, by default about 15 minutes max within a site and between sites according to the site replication intervals set by the system's administrators (very much like Exchange).

But how do you replicate an object that isn't there anymore? The way AD does it (and Exchange too) is to create a tombstone and copy the tombstone to every DC. The tombstone points to the deleted object and "deletes it". Periodically a background process collects all the tombstones older than 30 days and gets rid of them.

These are why you can't restore an older AD instance with the deleted object and have the old object magically appear again. The other DCs will have the tombstone for that object and it will show a higher USN than the object in the restore, so it too will be tomb stoned when the DC gets caught up with its neighbors.

In an authoritative restore, you identify an AD object (domain to user) as "authoritative" in the domain. This means you tell AD that this (version of the) object has authority and is to be replicated, superseding tomb stoned versions currently existing in the AD. (Many Exchange admins have told us they would love it if Exchange did this).

NOTE: Each of the above scenarios assume that there is at least one functional, up to date DC for the domain of interest online and available to finish the recovery. For this reason (and others), we recommend that no production domain ever be supported by less than two DCs.

T- Please see the - Recovery.doc file

3. **Will all agencies participating in the Active Directory world be required to install the same version of Windows 2K?Exchange?**

B - Each agency can go at their own pace to deploy their Active Directory or desktops. As long as there is a single forest, there are no concerns with the Global Address List with Exchange and agencies will be able to interoperate between Windows 2000 Active directory configuration as well as agencies with NT4 domain(s).

G/T – An agency can go to whatever version of Windows 2000 that they wish (including future versions of the product), The State Enterprise Administrator Group has plans, however, to put a mandatory requirement for ALL participating agencies to maintain same SP levels and versioning. (Primarily for support issues).

"Joining the Forest" means upgrading the NT4 domain controllers ONLY. NO member servers or NT4/Win9x workstations must be upgraded to join the domain. NT4/Win9x clients do not have knowledge of OUs or group policy, though, so at the point an agency wants that functionality, the stations will need to be upgraded. There is an AD client for NT4/Win9x that shows the OU structure and allows users to search it, but group policies such as software push requires Windows 2000 clients.

This means that once the root servers are up, an agency can upgrade its domain controllers (joining the forest), and upgrade its workstations and/or member servers in any order that makes good business sense. Existing Exchange 5.5 servers can be maintained as long as needed.

Native and Mixed mode Exchange environments will require a certain level of versioning and functionality for things like Universal Groups (used for Public Folder Permissions). Exchange can also be version agnostic between 5.5 and Exchange, however you must note that ONLY one Exchange 2000 organization can exist in the Forest. So 5.5 can exist fine, but no upgrade to Exchange 2000 is available unless your 5.5 org is a current participant of the Exchange hub and the Schema (/forest prep) has been modified. Agencies can upgrade to Windows 2000 and/or Active Directory (joining the forest) at any time and in any order. Exchange 2000 and Exchange 5.5 can peacefully coexist based on information presented above.

There is an Active Directory connector that will connect Active Directory to Exchange 5.5 that will perform a two-way sync between AD and Exchange 5.5 to keep the GAL up to date and synchronized. You can also set up trusts between Windows 2000 domains and NT 4 domains as needed or required for interoperability

NOTE: Exchange 2000 can't be installed until the root domain is available.

4. **How many forests exist at Microsoft? What was the basis for deciding that a single forest approach did not work? How did Microsoft decide to segment the individual forests?**

B - The main reason that there are three external forests at Microsoft is that the three units have no business reasons to be joined together. The users are different with different needs and requirements and there are no applications that are shared between them (like Exchange) that would need a global catalog to contain membership of all the forests.

G - There are three forests outside of Microsoft. They are Corp.Microsoft.com, Msn.com, and Hotmail.com. There are several internal forests within Microsoft for development purposes. One for Microsoft corporate (~40,000 users), one for MSN, and one for Hotmail. The decision to use separate forests for these three was driven by business requirements—even though Hotmail and MSN are owned by Microsoft, they operate as completely separate business entities with no operational or business requirement to share resources. Forest design theory says you draw forest boundaries around entities that are part of the same business and between those that are not.

The developer forests exist so the Microsoft Developer employees can play with the schema. You don't want schema changes going to the production network until they are clean and well tested, so that work has to be done in its own forest. The state will undoubtedly have one or more developer forests for this same reason.

5. The state LAN infrastructure and administration is distributed to the agency level and in large agencies, to the section level. Does Microsoft view the current state design of a single forest that includes all state agencies as a viable solution in this type of environment?

B/G - Yes, this was the exact thought that Active Directory was designed to work in. There are tools built into Active Directory that allows the delegation of authority to take place down the lowest level in the directory thus allowing administration tasks to be set to only the levels needed without having to give more rights than needed to perform tasks.

T- Delegation of authority wizard allows delegation of administration rights down to the OU level. Domain Administrators still have the rights they had in NT 4 and should still be a limited group of people that have a need for this right. Also, domain administrators should have two accounts (even in NT 4) and only use the account that has the Domain Administrator rights when performing a task that requires this right.

6. What recommendations does Microsoft propose to mitigate the risk of any one agency creating problems/issues/outages for the other agencies?

B – A technically competent schema management team that represents all stakeholders should inbound and evaluate schema change requests, approve or deny as appropriate, implement the changes approved. Draw domain boundaries between agencies to isolate administrative areas from each other

G - Keep the number of Domain Administrators, Schema Administrators and Enterprise Administrators to an absolute minimum.

T - To help keep accounts secure it is recommended that accounts have to change passwords at shorter (45 days or so) intervals, You can also set passwords to strong (8 or more characters), don't allow any of the last 10 (or so) passwords to be reused, and enforce use of mixed case and character passwords (caveat here is to not make it so difficult that the users ends up writing the password down on a sticky note by the monitor).

7. How consolidation can be set up to ensure that the risk is mitigated?

B/G - Mitigating risk of interagency problems is mostly a process of collaborating on shared needs and developing administrative processes and controls that leverage the administrative capabilities of Active Directory. Basically, the agencies need to get along and to agree on how the shared component of Active Directory (schema and infrastructure) should be managed. Once this is in place, drawing domain boundaries will isolate agencies from each other's day-to-day operations.

T - It is a best practice, when upgrading domain controllers, to bring an old computer on line as a BDC in your current domain that you are going to upgrade. After the Sync of the SAM database occurs, take the computer off line and store it someplace safe that you can get to it later (if needed). Then upgrade your DC's to Windows 2000 and use the Active Directory wizard to join the domain you are looking to join.

8. What are the advantages of a single state forest? Can a benefits analysis based upon potential advantages vs. risk be put in place?

B/G - Most of the early business advantages will happen intra-agency. Only over time will the interagency benefits unfold, as workers and IT professionals begin to see new ways of using this cheap, ubiquitous storage system. The price you pay (compared to a forest per agency) is that the agencies need to figure out how to manage the schema and infrastructure. Once that is in place, the agencies can run their own domains autonomously

The enterprise applications that utilize the Active Directory will be much easier to manage and create if there is only one directory. You can still maintain the granular security through domains and keep everyone from data that they should not have access to. The ability to have different agencies share information (if desired) and the flexibility to have a single statewide repository in many cases will far outweigh the risks.

At the core, a single forest will give state business managers a far more powerful and useful compute infrastructure than they have now. Business managers will be able to try out ideas that require a change in the IT infra with virtually no risk. It will be simple to do things like get new applications to workers that need them, and very straightforward for IT staff to, for example, implement a new organization design. A single forest makes it possible to share information in new ways, with much higher accuracy and at reduced cost, without building new systems. One of the less obvious short-term advantages of a single forest will be to force collaboration around inter-agency information sharing needs. Longer term advantages include much faster access to information, far easier sharing of operational skills, and a much more pyramid-shaped support structure (delegation of administrative control)

T- Domains are still as secure as they were in NT 4.0 and in many ways even more secure. Although there is transitive trust between domains in Windows 2000, you can set the Access Control Lists to block any unwanted access into your domain that you desire. As an additional level of security, you can turn on IP Security between domains (or sites or even two computers) to allow only encrypted data to/from specified computers within the forest thus tightening security even further.

9. If the state decides to proceed with this design, what is the advantages to agencies that move to WIN2000 in the near term knowing that many agencies will be able to migrate to WIN 2000 for several years or even longer?

G The agencies that go right away will immediately start to see manageability benefits such as, easily deploying applications, desktop lockdown, granular control of authority, and many other benefits. They will still also be able to communicate fully with the domains that decide to wait. The agencies that wait will also be able to keep doing things exactly as they are doing currently, but have the open option of joining at any time they wish and start gaining the benefits when they are ready. There is no risk for agencies that wait to deploy, just additional benefits for the ones that go sooner.

10. Have other organizations put a single forest in place utilizing a multiple administration model? If so, who, how is it working, where is the demarcation between the distributed/centralized administration?

G - Most organizations have gone to a model like this. United States Air Force is one of the largest production rollouts of this type, but TRW, Wells Fargo, and Lockheed Martin, as well as many others are some of our customer examples.

11. Do agencies have options to participate (or not) without impacting email and document sharing?

G/T-Yes. Agencies can join the forest or not, upgrade their desktops or not, or continue to use Exchange 5.5 without creating any issues for themselves or agencies that choose to go forward. All existing functionality will continue to exist as agencies move forward. Agencies running on their current platform will not have access to the new functionality until they upgrade. If however, a multi forest model is decided on, there will be additional overhead needed to gain this type of sharing. E-mail used the Global Catalog for the Global Address list as well as document sharing between forests. If agencies are in separated forests there will be a need to keep all user account information synchronized between forests. This can be achieved through a service like Microsoft Meta Directory service, but this is even more overhead and another directory to maintain. Not to mention that any agency currently participating in the Exchange 5.5 hub will loose the ability to participate on that hub (Global Address List) if they move to their own forest And upgrade to Exchange 2000. They would need to break the Existing 5.5 org and use something like MMS to re-gain connectivity.

12. Will the business model developed by the Windows 2000 committees help agencies decide if and when to participate in the single forest?

B/G-While we can't speak for the committee, and the committee can't speak for the technical or financial readiness of any agency, other groups with similar responsibilities have (and are now) developing implementation templates and readiness guidelines to provide exactly this help. A well designed Active Directory and Windows 2000 implementation plan lets diverse business units continue to engage at their current level while making the way clear for them to join the new structure when the agency can make its own business case to do so. From a Microsoft perspective, this is a good idea.

13. What are the statewide infrastructure risks and operational problems that will result if for instance 1/2 of the cabinet agencies participated and the other 1/2 do not? What if DOP does not participate, but DIS, OFM and General Administration participate?

G The agencies that go right away will immediately start to see manageability benefits such as, easily deploying applications, desktop lockdown, granular control of authority, and many other benefits. They will still also be able to communicate fully with the domains that decide to wait. The agencies that wait will also be able to keep doing things exactly as they are doing currently, but have the open option of joining at any time they wish and start gaining the benefits when they are ready. There is no penalty for agencies that wait to deploy, just additional benefits for the ones that go sooner however, we believe that any group of agencies that choose to go forward should as a matter of professional IT responsibility design their implementation in such a way that agencies joining in the future will find the process straightforward, well understood, and clear from a cost-benefit business perspective.

14. When will specific business (non-technical) information be available for managers (non-technical) to decide if their agency should or should not participate?

B-This, we believe, is the appropriate responsibility of the Steering Committee to articulate the business case (pros and cons) and the technical working group to develop the operational roadmap.

Note: "Top 10 Reasons to Go with the Server Family.doc"

15. I still do not see specific business (non-technical) information for me (as a non-technical Manager) to decide why DOP should or should not participate.

B - Please read "Top 10 Reasons to Go with the Server Family.doc"

16. This document seems to have a bias for the technical migration to Active Directory- (which is needed), but there must be more clarity for:

a. State infrastructure efficiencies and economics of scale (cost and resources) for statewide participation.

G In general, the incremental cost for Windows 2000 is an investment for the future in order for the state to leverage the data sharing capabilities of the Active Directory for existing and future applications, which ultimately will reduce costs of maintaining at a minimum multiple employee directories servicing these applications. The overhead of Windows 2000 and Active directory will be less that your current NTT 4 environment. You will be able to reduce the number of domains and domain controllers needed for the support of so many domains. Your overall administration costs in most cases will drop as well. There will be an increase in tasks that are not included in NT 4, like schema administration, but the schema does not require a lot of maintenance, just changes as required for the states business model. There will also be work involved to get the design right. AD planning is DEFINITELY MORE complex than NT 4 and doing it right from the get-go is important to realize the benefits. Having a statewide participation in a single forest allows the agencies to pull their best technical resources together. Single forest means that only a single schema needs to be maintained, thus eliminating the need to have each agency plan and manage their schema administration.

b. If we do not have the resources to move for 2 years what happens?

B - The need for fast service and better information sharing may become mandatory rather than desirable. Active Directory is one solution to this issue that will already be in place to leverage.

G - Nothing technically will happen if the wait is 2 years for the migration. Things will remain as they are today and the state will not start gaining some of the benefits of having a Windows 2000 platform that reduces management overhead and increases security. The state will also not be able to move to Exchange 2000 until there is at least a minimal Active Directory in place. So again, nothing bad or good will happen.

c. How can Active Directory (Single State Forest) help, hinder or complicate existing technology applications that exist today? For example:

- ✓ **OFM's Travel Voucher Intranet application.**
- ✓ **L&I's HR Cafe - An agency unique HRIS that includes information and transactions for all L&I employees.**
- ✓ **GA's in-development TUPS Application (I am not familiar with this App so may have misread his writing) for on-line purchasing and processing for central stores items.**

G - Specific Applications need to be tested. Generally, applications running successfully under NT4 will run under Windows 2000, testing is always needed to know for sure.

d. The ability to have an efficient and stable e-mail/document sharing conduit between state government agencies?

G Single forest will not hinder the single statewide e-mail system. In fact the overall maintenance of the statewide e-mail system will start to decrease as the Active Directory integration increases due to the Global Catalog acting as the Global Address book. If a single forest model is not chosen as the core design, the same would not apply, please see notes above.

e. For agencies using the DIS backbone?

G -If it is on connectivity, there would be no change from the way you connect today. There are some new features available in the Windows 2000 environment.

f. For agencies using an Internet Service Provider?

G- Connections to ISPs work the same way they do today

Microsoft Corporation & Netdesk Corporation Contacts:

Microsoft	
Peg Souders Microsoft Account Executive State & Local Government Washington State & Alaska 425/705-1877 pegs@microsoft.com	Allen G. Abrahamson Microsoft Senior Systems Engineer Industry Solutions Group Central and West Region (818) 599-7415 aabraham@microsoft.com
Caesar Cunningham Consultant Microsoft Consulting Service PacWest (425) 705-1871 X51871 caesarc@microsoft.com	Jane Rasmussen Managing Consultant Microsoft Consulting Services MCS Federal (425) 705-1751 janer@microsoft.com
Todd Shelton President – Technical Business Consultant Netdesk Corporation (206) 224-7674 Todd.Shelton@netdesk.com	Jeff Langford Microsoft Systems Engineer State & Local Government West Region (425) 705-1779 jefflang@microsoft.com